STANDARDS – INFORMATION TECHNOLOGY 0950
(No.13 October 2002)

STANDARD HARDWARE/SOFTWARE LISTS 0950.1
(No.13 October 2002)

(See Hardware/Software Lists)

DESKTOP COMPUTERS 0950.2
(No.13 October 2002)

When replacing a Personal Computer (PC) it is not necessary to purchase a new monitor with the system. If the current monitor works and meets the end user's needs, the Purchase Request should include the desired system to be purchased with a notation stating "without monitor." To obtain the proper configuration for the staff member who will use the PC, customizations for other components may be applied as well. Examples include either adding or subtracting the following: CD Reader, CD Read/Write, DVD Player, Zip Drive, Memory and Video Cards.

WIRELESS STANDARDS 0950.3
(No.29 March 2012)

REV

PURPOSE
This compliance standard defines the wireless network structure for CAL FIRE and assigns responsibilities for the use and administration of wireless services.

SCOPE
- This standard pertains to all wireless products used to conduct CAL FIRE business.
- This standard is required to be used by all CAL FIRE locations and staff.
- This standard does not apply to radio or microwave infrastructure.
- This standard does not apply to 3G or 4G smartphone, hotspot, or tablet products.

TYPES OF WIRELESS PRODUCTS COVERED BY THIS STANDARD
- Fixed Hotspot (Non WAN Connected)

  This type of wireless product provides wireless connectivity to the Internet for sites that are not WAN connected. Security considerations are less than a WAN connected hotspot as enterprise assets cannot be directly accessed without the use of other security products.

- Point to Point

  This type of wireless connectivity is designed to connect buildings on a compound to each other to provide a Local Area Network in a fixed location where cabling is not a practical solution. This connection type only allows secure transmissions between two end points, and no other connectivity is allowed.

- Fixed Hotspot (WAN Connected)

  This type of wireless connectivity provides connection to computers and devices that need access to the CAL FIRE enterprise computing environment where a high level of secure access is needed.

STANDARD STATEMENTS

- All wireless products and services must be approved for use by the departmental CIO.
- All wireless infrastructures will be installed and maintained by CAL FIRE Information Technology staff or approved partners. This includes the procurement, installation, and maintenance of all equipment.

Addendum A
CAL FIRE Wireless Technical Specifications
For Fixed Hotspot - Non-WAN locations

Note: These technical specifications change regularly. To ensure compliance, please contact Information Technology Enterprise Architecture

The following is a list of security requirements to implement at CAL FIRE "remote" (non-WAN connected) sites, such as Stations, Camps and Airbases.

1. Change the default SSID (aka wireless network name).
2. Disable SSID Broadcast. NOTE: Disabling SSID broadcast means that every wireless client must be manually configured, i.e. they won't automatically find the SSID/wireless network name.
3. Change the default password for the Administrator account.
4. Use the highest encryption algorithm possible: USE WPA or WPA2, preferably WPA2 only. (WPA2 is also sometimes called 802.11i). The minimum for CAL FIRE sites is WPA2. At home, if WEP is the best available, change the WEP encryption keys periodically. Be advised that WEP is so easy to hack/crack that it is worthless.
5. Use complex passwords/passphrases, 15 characters minimum.
6. Change the SSID once per year.
7. Change the Administrator password once per year.
8. Don't use the same phrase for SSID, WPA passphrase, or admin password.
9. (optional) Enable MAC Address Filtering, and allow only those MAC addresses of the PCs in your office. NOTE: If you have laptops coming and leaving all the time, this can be VERY labor intensive!

Note 1: When purchasing new equipment, ensure that it is 802.11n and IPv6 capable.
Note 2: For many manufacturers, WPA-PSK or WPA2-PSK (PSK==Pre Shared Key) is the terminology used for the type of security required by policy, i.e. it requires a passphrase. Some vendors use the terms WPA and WPA-Enterprise; in this case, you'll want to use WPA2. (WPA-Enterprise requires a RADIUS server to validate login & password).
Note 3: For Microsoft XP: Ensure that wireless laptops have the MS XP built-in firewall enabled; there is a known vulnerability that enables hackers (and innocent bystanders) access to the laptop via wireless. Another way to thwart this is to check the "Access point (infrastructure) networks only" box under Start->Control Panel -> Network Connections -> Wireless Network Connection -> Properties -> Wireless Networks -> Advanced.

Addendum B
CAL FIRE Wireless Technical Specifications
For Point to Point Connectivity

Due to the varying conditions that go into designing a point-to-point wireless connection, this type of wireless connectivity will have to be dealt with on a case by case basis by CAL FIRE ITS Enterprise Architecture.

Addendum C
CAL FIRE Wireless Technical Specifications
For Fixed Hotspot - WAN locations

Cal Fire currently uses a Cisco proprietary system that uses a central controller to control and configure all access points. The product uses Lightweight Access Point Protocol (LWAPP), and operates on both 802.11a (5Gz) and 802.11b/g (2.4Gz) frequencies. All staff must contact ITS Enterprise Architecture prior to the design and purchase of any wireless equipment for this type of wireless connectivity.

Note: this system is aging and due to be upgraded in 2012, and does not support the WiFi 802.11n standard.

Further technical discussion: this system employs high security features:

- Lockout after a given number of failed connection attempts
- 802.1x, which requires a valid Active Directory login and password (and encrypts them over the airwaves)
- A special Microsoft security token that helps ensure the PC/laptop has been authorized to connect to the CAL FIRE network

COPIER SCAN TO EMAIL IS NOT PERMITTED 0950.4

(No.28 MAY 2011)

CAL FIRE staff wishing to deploy “Standard Procurement List” select copiers with network and scanning capability must configure those copiers to send scanned documents to designated workstation folders and not directly to the CAL FIRE email system. This configuration will greatly reduce the risk of unintentionally inundating the email system with large files.

(see next section)

(see HB Table of Contents)

(see Forms or Forms Samples)